A MARKET RESPONSE TO THE EUROPEAN UNION DIRECTIVE ON PRIVACY

Paul Rose[*]

U.S. data marketers argue that electronic commerce can only flourish if allowed to develop without restraining legislation. Privacy enthusiasts counter that the development of e-commerce is presently hampered by public fear over the uses of private data transferred through online transactions. The United States and the European Union share a commitment to the development of electronic commerce, but have approached the problem of data protection very differently. The EU has promulgated a comprehensive data protection regulation, The European Union Directive on Data Protection, while the United States prefers a market-driven approach, combining legislation, regulation, and, predominantly, self-regulation.

In this Comment, Paul Rose proposes a market solution--the creation of a new privacy market, that satisfies the U.S preference for an entirely industry-generated solution to the problems of data transfers, yet also satisfies the demands of the EU Directive on Data Protection

---

[*] J.D. Candidate, UCLA School of Law, 2001; B.A., Brigham Young University, 1995. Special thanks to Professor Richard Steinberg, who provided the seminal concept for this comment. This comment received the 1999 Morris Greenspan Prize as UCLA School of Law's best paper on the topic of international law.

> "Because this technology knows no borders, it is far better for the market to respond than for governments around the world to take action."
>
> --U.S. Commerce Secretary William M. Daley

INTRODUCTION: A PRIMER ON U.S. AND EU POSITIONS ON DATA PROTECTION IN INTERNET CONSUMER TRANSACTIONS

In 1995, the European Union harmonized data protection standards across its member states through the Directive on Data Protection[1]

[1] *See Council Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995 O.J. (L281) 31 (Nov. 23, 1995)

(Directive). The Directive requires that all member states enact data protection measures,[2] and also requires that non-EU countries

<http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html> [hereinafter *Directive*]. I use the somewhat dehumanizing term "data subject" throughout this paper to describe individuals engaging in online transactions. I find this EU and Organization for Economic Cooperation and Development (OECD) term to be an appropriate descriptor because it focuses on the proprietary relationship between a person and her data.

[2] The OECD has outlined eight basic "privacy principles" to govern personal data transfers:

> 1. Collection Limitation: there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; 2. Data Quality: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date; 3. Purpose Specification: the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion or change of purpose; 4. Use Limitation: personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law; 5. Security Safeguards: personal data should be protected by reasonable security safeguard against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data; 6. Openness: there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller; 7. Individual participation: an individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended; 8. Accountability: a data controller should be accountable for complying with measures that give effect to the principles stated above.

OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); *see also* OECD, Working Party on Information Security and Privacy, Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks (DSTI/ICCP/REG(98)12/FINAL) 10-11 (1999) [hereinafter OECD Inventory]. The Federal Trade Commission has distilled these principles into four pairs of principles: Notice/Awareness, Choice/Consent,

receiving personal data[3] transfers from EU countries provide an "adequate" level of privacy protection for European personal data. Failure to provide adequate protection will result in member states taking "the measures necessary to prevent any transfer of data of the same type to the third country in question,"[4] including cutting off data flows to "data protection outlaw nations."[5]

The European Union and the United States both have deep commitments to the development of electronic commerce, and are working to insure an uninterrupted flow of information. However, the EU and U.S. approaches to data protection differ significantly. While the European Union favors comprehensive data protection regulations, the United States prefers a "sectoral" approach, combining legislation, regulation, and, predominantly, self-regulation,[6] on the premise that "private efforts of industry working in cooperation with consumer groups are preferable to governmental regulation."[7] In response to the requirements of the EU Directive, the EU and U.S. (through the efforts of the Department of Commerce and U.S. businesses) are developing the "International Safe Harbor Privacy Principles,"[8] a basic self-

Access/Participation, and Security/Integrity. *See* FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7-11 (1998) [hereinafter PRIVACY ONLINE].

[3] "'Personal data' are the data relating to any identified or identifiable individual (the 'data subject'). Individuals are identifiable not only by means of their name but also by their pictures, by their telephone number, by some special identification number etc." European Union DG XV, *Data Protection: Background Information* (visited Nov. 11, 1999) <http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/info.htm>.

[4] *Directive*, art. 25.4, *supra* note 1.

[5] Paul M. Schwartz, *European Data Protection Law and the Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 484 (1995).

[6] The U.S. also relies on a very few sector-specific statutes, such as the Fair Credit Reporting Act, 15 U.S.C.C. § 1681 (Supp. 3), and the Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1994).

[7] William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (visited Sept. 30, 1999) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> [hereinafter *Framework*].

[8] The term "Safe Harbor" does not refer to a safe harbor for European citizens, but a safe harbor for companies who comply with the principles, and are thus presumed to provide "adequate" protection for personal data transfers. *See* Dep't of Commerce, *International Safe Harbor Privacy Principles* (visited Sept. 27, 1999) <http://www.ita.doc.gov/ecom/shprin.html> (draft of Apr. 19, 1999) [hereinafter Safe Harbor Principles].

regulatory framework for U.S. businesses seeking to comply with the Directive.

The current U.S. self-regulation model has yet to resolve many of the domestic privacy concerns that worry Internet users,[9] and some Europeans have expressed skepticism that the Safe Harbor Principles will provide adequate protection for trans-border data flows. This skepticism stems from concerns over the advantages U.S. businesses enjoy over consumers under the current scheme. Online businesses have access to powerful information collection technologies that allow them to create valuable personal information profiles--the hot commodity in a burgeoning personal data market--for use in various business operations from marketing to risk management. These businesses (especially data marketing companies whose primary business is to track and sell personal data, such as Engage Technologies, Acxiom, Doubleclick and Clickstream) thus have a strong incentive to preserve a deregulated forum where they can maintain control over the lucrative personal information marketplace. But, as Joel Reidenberg explains, "a marketplace can only function efficiently if there is transparency; citizens must be able to identify the collectors and users of their personal information. However, for personal information, the natural tendency of the marketplace is to obscure its treatment."[10] Because many e-commerce businesses are unwilling to deal transparently,[11] and do not wish to give up

[9] Forrester Technographics reports that two-thirds of online shoppers feel insecure about exchanging personal information over the Internet, limiting the development of electronic commerce. *See Forrester Technographics Finds Online Consumers Fearful of Privacy Violations*, BUSINESS WIRE, Oct. 27, 1999. *See also* Privacy Exchange.org, *1998 Privacy Concerns & Consumer Choice Survey, Executive Summary, P&AB Survey*, PRIVACY & AM. BUS., Jan.-Feb. 1999, at 1; <http://www.privacyexchange.org/iss/surveys/1298exec-sum.html> (reporting that 82% of those surveyed believe that consumers have lost all control over how companies collect and use personal data); AARP, *AARP Members' Concerns About Information Privacy* (Dec. 1998) (reporting that 78% of respondents found existing legislative measures to be inadequate to protect privacy).

[10] Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERK. TECH. L.J. 771, 775 (1999).

[11] As Jerry Kang notes, market solutions tend to ignore heavy transaction costs associated with creating a transparent market. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1248 (1998).

innovative, powerful marketing tools,[12] consumers are invariably the losers in the data market.[13] Data subjects are typically required to sacrifice valuable private data without compensation as a condition of transacting online, and are not able to "buy back" their personal information once it has been given up. Some scholars have suggested that the market's failure necessitates a legislative response.[14] However, because of the deep U.S. commitment to self-regulation and to the Safe Harbor Principles, comprehensive privacy legislation is unlikely, and, as I argue, unnecessary. Although the *data* market has failed consumers, privacy concerns can still be resolved through market forces--through the creation of a *privacy* market.

In this paper I discuss the privacy market solution to data protection, which would further U.S. market preferences, yet offer the personal data protection required by the EU Directive. In Part I, I outline the privacy market solution: the privacy escrow system. In Part II, I discuss how this solution satisfies the European Union Directive. In Part III, I discuss how this solution addresses U.S. concerns.

I. THE PRIVACY PROBLEM AND THE ROLE OF THE PRIVACY ESCROW

The EU Directive on Data Protection covers all types of data transfers, including transfers involving medical information, personal information gathered through loan applications, employee information

[12] Data collection is big business: in 1998, the gross annual revenue of companies selling private data reached 1.5 billion. *See* In Re Trans Union, FTC Docket No. 9255, at 53 (July 31, 1998), *available at* <http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf> (visited Mar. 28, 1998).

[13] Private data, while having some value for the consumer, may have more value to the business tracking the information. For example, I may not value the datum that I am a law student, since the information is easily available. However, the information may be of some value to the auto manufacturers, for example, who anticipate that after graduation I will find employment and will want to find a way to spend the last few dollars available after student loan payments.

[14] *See* Kang, *supra* note 11; Reidenberg, *supra* note 10.

gathered by human resources departments, and information obtained through online transactions. Inevitably, businesses digitally file these data, efficiently manipulating the information in order to create a detailed personal "file" (a technique known as "profiling"). The ability to easily manipulate sensitive data and transfer the data on to third parties in third countries has focused attention on an increasingly important international data transfer system: the Internet. Although basic telephony and paper data transfers implicate important data concerns, the Internet and other forms of digital information transfers have become the most efficient and rapidly expanding means of personal data transfer. Accordingly, I limit my focus in this paper to Internet data transfers.

A. *Privacy in Online Transactions*

1. Defining Privacy

Privacy as a general right or value includes several related notions or "facets."[15] Among these we may include (1) *information privacy* (concerning personal data such as credit or medical information); (2) *bodily privacy* (concerning the protection of a person against invasive physical contact); (3) *privacy of communications* (concerning telephone, mail, email and other forms of communication); and (4) *territorial privacy* (concerning the protection of domestic or other types of "personal" space). I will primarily focus on information privacy and privacy of communications, since these are the facets of privacy typically implicated by the EU Directive and in Internet activity. When I discuss "privacy" throughout the paper, I generally refer to information privacy and communications privacy concerns. Privacy defenders often label privacy as a property interest. This

[15] *See* David Banisar & Simon Davies, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice* (visited Dec. 12, 1999) <http://www.gilc.org/privacy/survey/intro.html>. I do not presume that the definition offered here perfectly or even thoroughly describes the nature and scope of the concept of privacy. However, for the limited needs and scope of this paper, the definition should adequately frame a common understanding of privacy.

notion has intuitive appeal--my personal data *belong* to me, and I should have sole decisional rights as to the disposition of my personal data. Professor Jerry Kang notes that

> [p]rivacy enthusiasts insist that the individual self-evidently owns her personal information. Therefore, the information collector should not be able to make use of that "property" without permission. Unfortunately, what is self-evident for some is question-begging for others. Information collectors retort that the information was generated in a mutual interaction, in which the individual and the information collector were equal participants. Why then should the individual have preferred rights over what was jointly produced?[16]

While privacy enthusiasts and information collectors disagree on whether *post*-transaction information remains the sole property of the original owner, or that data subjects and data collectors co-own the information, suppose we stipulate only that *pre*-transaction information is solely possessed by the data subject. This assumption, too, "could easily be defeated by the realities of modern transactional life."[17] Individuals asserting a property right over their personal information would undoubtedly value the information differently. Routine transactions, such as obtaining a loan, applying for credit, or setting up telephone service would be inefficiently complicated as individuals haggled with businesses over the value of commonly transferred personal information, such as a social security number.[18] Because the property rights approach appears impractical, "anonymity [the approach I forward in this comment] may be the only technique of resistance to profiling (short of civil disobedience or outright surrender) available to the average citizen."[19]

The creation of a property right over personal information is not necessary to justify the creation of a privacy market. The commodity

---

[16] Kang, *supra* note 11, at 1246.

[17] A. Michael Froomkin, *Regulation of Computing and Information Technology: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 492 (1996).

[18] *See id.*

[19] *Id.* at 493.

of the market that I describe in this comment is not personal information, but *privacy* itself, achieved through anonymous communications and transactions.[20] In some cases, individuals may be able to bargain with their personal data.[21] However, because of the impracticality of valuing property rights on personal information, efficient control of personal information is more likely achieved by paying a premium on transactions to insure that personal data remain private,[22] than by engaging in wasteful bargaining over the value of various personal data. The privacy market approach does not seek to quantify the value of personal data, but the value of privacy.

2. Private Data Transfers

Having briefly described a definitional foundation for a discussion of privacy and private information, I now move to a description of the ways in which private information is transferred and collected in online transactions and communications. My scope covers three primary categories of cross-border personal data flows for which there exists, or could exist, an adequate privacy market response. These three categories of data flows reflect the range of increasingly

---

[20] I view anonymity as a means of insuring privacy, rather than as a synonym for privacy. Privacy is achieved through personal data control; anonymity, or selective anonymity, allows data subjects to maintain this control.

[21] *But see* Reidenberg, *supra* note 10, at 775 (arguing that "privacy interests are central to democratic governance and privacy has been hailed as a necessary condition for participatory governance. In contrast, totalitarian governments prefer the surveillance state. Indeed, a democratic government typically does not sell basic political rights" (citations omitted)). *See also* ALAN F. WESTIN, PRIVACY AND FREEDOM 23-26, (1967). However, inasmuch as private data is a property interest, the freedom to dispose of property conflicts with this notion. My own concern is not that individuals would wish to sell private information, but that they are able to sell the information in a well-functioning market, where they are able to command a fair price for the information, or would be able to pay a fair price to insure anonymity.

[22] Because the U.S. is unlikely to pass comprehensive privacy regulations, individuals will have to pay to insure the security of their data, even if they do have a property interest in their information. Under the current U.S. position, however, there is no protection of privacy as a property interest--individuals are unable to take a data collector to court in order to have the information remitted to the "owner." The U.S. does allow individuals a cause of action against companies that make inappropriate use of the information.

important online personal information transfers between EU member states and U.S. companies.

The first type of data flow occurs as companies collect information from an individual as she browses web sites. When an individual visits servers through Internet browsing activity, the server typically logs the URL[23] of the resource from which the request was made, and also logs the time of visit. The server may also set a "cookie," a file that logs information the client offers during her visit. The server then stores the cookie on the client's hard drive. The data collector server then accesses the cookie when a client returns to the site, and the cookie allows the server to personalize the information presented to the client. Although cookies typically contain only small, isolated bits of private information, companies sometimes agree to share information gathered through cookies, producing a mosaic of valuable personal information.[24]

The second type of data flow occurs through email systems. When email messages are sent they include a header, which identifies the sender, and which may also identify the sender's operating system. Anonymous re-mailers, which "re-mail" email messages through a series of servers in order to disguise the identity of the sender, answer this concern to the extent that the re-mailed messages are not ultimately traceable to the sender.[25] However, the abuse of re-mailers has created new concerns, as clients use the services to send offensive messages or mass mailings. Because of these abuses, some anonymous re-mailing systems have been forced to cease operation.[26]

---

[23] The "Uniform Resource Locator," or the "address," such as <http://www.law.ucla.edu>.

[24] For example, businesses may be able to determine what key word searches an individual conducted, what sites the individual visited, how long they lingered at certain pages, and what they purchased.

[25] Some anonymous re-mailers, such as the Hotmail Re-mailer, Anonymizer, and the Freedom Re-mailer, allow clients to send email through web pages, allowing complete anonymity. Other re-mailers send email through a series of servers, readdressing the message and resending several times before sending it to the ultimate, intended recipient. Examples of this type of re-mailer are Replay and Nymserver.

[26] The integrity of privacy escrows is essential to the viability of the privacy market, just as the integrity of bankers is essential to a fair and legal banking system. The use of anonymizing technologies must be balanced with law enforcement interests, and privacy escrows must insure that the escrow system is not used for illegal activities. *See infra* Part II.B.

Third, individuals reveal personal information when they purchase goods or services over the Internet. Electronic commerce transactions usually require credit card payments, which necessitate the disclosure of some personal information. For example, a credit card purchase typically requires a client to give his name and his billing address, and sometimes a telephone number and email address. Ideally, consumers should have the option of remaining as anonymous as if they had paid cash in a face-to-face transaction; in effect, the online transaction could be even more anonymous than paying cash to a store clerk, since there would be no visible connection between a purchaser and a product.

3. The Data Market

To the extent that data subjects and online businesses bargain over the rules for these three types of data transfers, online businesses dominate the bargaining process. Typically, no bargaining occurs between the business and the data subject over the value and use of personal data.[27] The data subject usually gives up private data at no cost[28] to the data collector, as through email or browsing activities. Likewise, a data subject purchasing products over the Internet gives up private information as part of the transaction through payment mechanisms or simply by the products she purchases. Data collectors are able to sell this information in the data market with no "royalty" payment to the data subject.

So far, attempts to insure privacy in the data market have proved unsuccessful because the self-regulatory model typically relies on

---

[27] As Professor Jerry Kang argues, individual contracts between businesses and consumers are not feasible because of prohibitively high transactions costs. *See* Kang, *supra* note 11.

[28] Businesses may claim that the cost of the data is built in to the general transaction cost. Such a claim would be difficult to refute without analysis of a particular business' pricing models, although I am reasonably sure that such an analysis would reveal no "private data" component. A secondary privacy data market would ensure accurate pricing of private data by forcing businesses to openly bid for private data. For example, a company might offer a 10% discount in exchange for information on spending habits.

contracts between data subjects and data recipient businesses.[29] Data recipient businesses have little incentive to contract when they are receiving valuable information at no cost or at a very low cost. The data market also fails to protect privacy because data subjects are typically unaware of data recipient use of private information,[30] and would incur and impose[31] significant transaction costs in discovering this information and crafting contracts with individual data recipients.[32] The data subject's inability to control the use of their data, a result of data market inefficiencies, has brought calls for legislative action.[33] However, as Andrew Shapiro notes:

> [I]n the current deregulatory climate, the Clinton Administration and some privacy defenders are taking a different approach. They're calling for the creation of a market for privacy to compete with or complement the growing market for personal information. (A report released in April by a presidential advisory panel, for example, mentioned "the intriguing possibility that privacy could

---

[29] "Model contracts" have been offered as a possible solution. *See* OECD Inventory, *supra* note 2.

[30] Surveys show that data subjects are concerned that their privacy may be compromised through Internet transactions, but data recipients have little or no incentive to inform data subjects of the exact use of their private data, so data subjects are generally unaware of the extent of the data recipients' private information holdings, nor how the data recipients use this information. As Joel Reidenberg stated, "a marketplace can only function efficiently if there is transparency; citizens must be able to identify the collectors and users of their personal information. However, for personal information, the natural tendency of the marketplace is to obscure its treatment. This is a classic case of market failure." *See* Reidenberg, *supra* note 10, at 775.

[31] Data subjects would also increase product and services costs by imposing transactional costs on data subjects. Duncan MacDonald, a Citicorp executive, states that

> Most companies, even in a highly competitive market such as consumer financial services, must obtain and use certain data in relatively standard ways in order to provide the requested services efficiently, and it would be wholly impractical for such companies to collect and process data according to a large number of variable protocols, depending on variations in particular contractual arrangements reached with individual consumers.

Duncan A. MacDonald, *Privacy, Self-Regulation, and the Contractual Model: A Report from Citicorp Credit Services, Inc., available in* National Telecomms. & Info. Admin., U.S. Dep't of Commerce, *Privacy and Self-regulation in the Information Age* (1997) <http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm >.

[32] For a detailed argument, see Kang, *supra* note 11, at 1246-60.

[33] *See* Kang, *supra* note 11; Reidenberg, *supra* note 10.

> emerge as a market commodity in the Information Age.") Just as there is demand for consumer data among profiteers, so there is a counterdemand on the part of individuals to keep that information private.[34]

Although data recipients are unlikely to develop a privacy market voluntarily, new businesses specializing in data control may realize the "intriguing possibility" of a privacy market.

B. *The Privacy Escrow*

The privacy market that I will describe requires a new transactional framework that allows a data subject control over private data throughout the transaction. A real property transfer framework, the escrow system, offers a useful core structure on which to base a consumer-oriented data control system. While the escrow system serves as a property transfer framework, and may implicate property theories inapplicable to the privacy market, we need only consider its value as a transfer system and as a market facilitator. However, although I limit the theoretical appropriation from the real property escrow framework, I also note that the privacy escrow will perform a much broader set of functions than the real property escrow. The basic escrow framework will require various additions, pieced together from other types of data protection services, in order to support the varied functions of the privacy escrow. In the following sections, I will introduce the concept of the privacy escrow, first by distinguishing it from the real property escrow system, then by elaborating on the additional functions or services that the privacy escrow can offer online consumers.

---

[34] Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet* (visited Nov. 23, 1999) <http://www.thenation.com/issue/970623/0623shap.htm>.

1. Real Property Escrows to Privacy Escrows

A real property escrow is a neutral third party that performs various functions to close a real estate transaction.[35] The escrow performs several functions, including securing the transaction by ordering and delivering a commitment for title insurance to the parties, ordering all necessary payoff statements and demands to clear the title, and preparing all required documents to transfer title. The escrow then receives all the necessary documents, funds, and signatures to close the transaction, then records and delivers the documents and transfers the funds.

Some important additions and modifications must augment the core real property escrow framework in order to create a useful privacy escrow framework. In this expanded framework, privacy escrow agents[36] will act as a buffer between data subjects and online businesses. Rather than merely collecting and transferring data and secured funds, a privacy escrow would (1) allow the customer to browse through the online "store" anonymously; (2) provide anonymous emailing; and (3) provide for anonymous transactions by (a) collecting all information produced in a transaction; (b) stripping away the private data; (c) securing the transaction; (d) sending only the essential transactional information and necessary funds to the original transacting business; and (e) arranging for anonymous shipping (or practically anonymous, since the address would be unavailable to online businesses, but not to the shipping company). In

[35] *See* Professional Escrow Services, Inc., *Frequently Asked Questions For Buyers, Sellers and Refinances* (visited Nov. 22, 1999) <http://www.professionalescrow.com/cust/3040a.htm>.

[36] Privacy escrow agents already exist in limited form. Some companies providing "internet escrow services" are D & M Internet Escrow Service, Inc. ("assists buyers and sellers in making secure transactions from internet sources"); i-Escrow, Inc. ("assists buyers and sellers in establishing a safe, efficient, and secure transaction environment"); Internet Clearing Corporation ("online escrow service that pays seller immediately upon verification of shipment and guarantees buyer's complete satisfaction"); SecureTrades.Com ("an escrow and merchandise holding service for individuals using auction and classifieds web sites"); and TradeSafe ("escrow service specifically designed to make online buying, selling, and trading safe and easy"). However, these businesses offer only a part of the services--assurance of payment through a third party--that I believe to be necessary to establish a working market for privacy. They make no claim as to anonymity.

return for the service, a consumer would pay a privacy premium--a small transaction cost--to the escrow agent.

2. Anonymizing Browsing and Email

Anonymous browsing already exists through Anonymizer,[37] a fee-based service[38] that allows clients to surf the web and send email anonymously. Anonymizer is currently improving its service[39] through European produced 128-Bit encryption software "distributed from a country with no cryptography export restrictions."[40]

Anonymizer, like Internet escrow services and anonymous cash services I describe in the following section,[41] offers an incomplete

---

[37] *See* Anonymizer.com (visited Nov. 23, 1999) <http://www.anonymizer.com/3.0/index.shtml>. Anonymizer offers various services, including anonymous surfing, email, web publishing, and dial-up services.

[38] Anonymizer's fee structure indicates that consumers are willing to pay fairly well for privacy. While Anonymizer offers some browsing and email for "free", premium anonymous surfing (which saves the user from Anonymizer advertising that pays for the free service) costs $14.99 for three months of service, dial-up costs $59.95 for 3 months of service, and anonymous web publishing goes for $29.99 for six months of service.

[39] An Anonymizer advertisement touts its soon-to-be-released Anonymizer Pipeline service:

> Anonymizer Pipeline will protect your Internet activity with strong SSLeay 128-bit encryption between you and our network. It will allow you to use email, news, and the Web anonymously and securely from your personal computer. Your connection provider, and anyone on the network between you and the Anonymizer subnetwork, will see only scrambled data. All your activity will appear to come from the Anonymizer subnetwork in California. Anonymizer Pipeline will also include a Surfing account for anonymous Web browsing.

Anonymizer.com, *Anonymizer Pipeline* (visited Nov. 23, 1999) <http://www.anonymizer.com/3.0/services/pipeline.shtml>.

[40] Anonymizer states that "Pipeline is a European product distributed from a country with no cryptography export restrictions, so you can download and use Pipeline legally from any country without cryptography import restrictions. Apologies to our French customers--complain to your government." *Id.* The Clinton Administration recently submitted a proposal to relax encryption regulations, although the plan fell short of privacy groups expectations. *See* Jeri Clausing, *Administration Releases Draft of Encryption Export Rules*, New York Times on the Web (Nov. 23, 1999) <http://www.nytimes.com/library/tech/99/11/cyber/articles/24code.html>.

[41] *See infra* Part I.B.3.

solution to private data transfer concerns. Anonymizer insures anonymity while browsing or sending email, but does not insure anonymity during online shopping, where data subjects transfer credit card information to retailers. A comprehensive private data solution must respond to all situations in which data transfers occur, combining Anonymizer features with anonymous cash services and internet escrow features to create an entirely anonymous transaction, with no data transfers except to the privacy service provider and shippers. A privacy escrow could provide such a service for a monthly fee to clients who browse the Internet frequently, and wish to send email anonymously. For clients who wish to use the service primarily for online shopping, a per transaction fee structure may be more suitable.

3. Anonymizing Payment

The essential aspect of the privacy escrow service is the opportunity for consumers to transact anonymously. A couple of previous efforts to anonymize payment have been moderately successful. One existing service, Mondex,[42] allows consumers to pay for products over the Internet using a smart card. Mondex offers some privacy through its transactions, but cannot offer anonymity since purchases are traceable by participating businesses and banks as the Mondex account logs the client's last 300 purchases by card number, price, and date.[43]

Another electronic payment system, ECash,[44] offers similar privacy protections. Under the ECash system, a customer places order at an online business' web site, and the online business transfers order

---

[42] *See* Mondex on the Internet (visited Nov. 23, 1999) <http://www.mondex.com/mondex/cgi-bin/printpage.pl?style=noframescash&fname=../documents/net2.txt&doctype=genp> (claiming that "no-one need know who you are when using Mondex. When goods and services are purchased using Mondex there is no record held of the transaction, allowing the user the privacy normally only afforded with physical cash.").

[43] *See* Privacy International, *Privacy International's Mondex Complaint Is Upheld: Electronic Cash Is Anything But Anonymous* (visited Nov. 23, 1999) <http://www.privacyinternational.org/issues/mondex/mondex_release.html>. *See also* Privacy International, *Response from Fair Trading Office on Complaint* (visited Nov. 23, 1999) <http://www.privacy.org/pi/activities/mondex/mondex_response.html>.

[44] *See* ECash.com (visited Nov. 23, 1999) <http://www.ecash.com/ecash1.asp >.

information to ECash over the Internet via a proprietary electronic commerce messaging protocol (ECMP). ECash receives the order information and routes a transaction authorization request to the customer's card system (e.g., Visa). The card system then contacts the customer's card-issuing bank and requests transaction authorization from ECash. When ECash receives the transaction authorization, it sends an ECMP message to the online business or distribution center authorizing the order. The online business then sends ECash an ECMP fulfillment notification, and ECash sends a settlement request to the customer's bank. The customer's bank then transfers the money to the business' bank account.

A privacy escrow system would operate in a transactionally similar manner. Like Mondex or ECash, there will be a record of a debit (the price of the product plus the service premium) and a credit to the business' account, and the purchase could be traced to the consumer only if a particular bank decided to share transaction records with a particular business,[45] and could match up a product with a consumer by price and date of purchase. However, the chances of the bank and a business finding each other by mining through the transactions is very remote. Also, the privacy escrow could make the task even more difficult by transferring funds in blocks,[46] a feature unavailable with the Mondex and Ecash systems. While this may not be a significant improvement over the Mondex and ECash systems, the ability to have products shipped to your home, under your own name, is a crucial distinction. With either Mondex or ECash, so long as a name and address (or an email address, or an Internet Protocol address to a server or station) must be supplied to have a purchase shipped to a

[45] In Britain, the Mondex system benefits from banking regulations ensuring a bank's duty of privacy toward a customers transaction information. In the U.S., consumers have some protection under the Electronic Funds Transfer Act, 15 U.S.C. § 1963 (1994), which requires banks to inform consumers of the circumstances in which automated bank account information will be disclosed to third parties in ordinary business transactions.

[46] A principal concern with anonymous payment systems is their potential use in money laundering schemes. The short answer to this problem is that a balance must be struck between law enforcement exigencies and privacy demands--essentially the same debate as recent arguments over encryption. The longer answer addressing whether federal regulators would require certain monitoring rights, and if so, to what extent, is beyond the scope of this paper.

customer, the business will be able to track the consumer. More importantly, anonymous payment is of little use if the consumer gives away his private data by browsing through the business' web site. A privacy escrow could thus offer a higher degree of anonymity than either Mondex or ECash.

Besides the anonymity that the privacy escrow enables, consumers will also benefit because private information, again in control of the data subject, will no longer be available to businesses at no cost. Businesses looking to streamline marketing efforts[47] would likely need to offer incentives in the form of discounts or free products in order to entice data subjects to give up personal information.[48] Thus, a fringe benefit of the creation of a privacy market is that it may also improve a data subject's standing in the *data* market.

4. Securing Transactions

Although online businesses will lose whatever value they attach to particular personal data, they too will receive a small benefit from a privacy escrow-enabled transaction. Because the privacy escrow will not forward any credits to the online business' account until they are assured payment through a credit to their own account, the privacy escrow insulates online businesses from all costs associated with failed transactions (e.g., a person uses a check card for a transaction but has insufficient funds or credit to consummate the purchase). To the extent that failed transactions create additional processing costs for the

---

[47] *See supra* note 20.

[48] For those interested in knowing what price basic private information commands in today's data market, visit <http://www.hugo.com/hugo_home_flash/main.html>, where your name, address, email, sex, and birthday entitle you to a free sample of "Dark Blue," Hugo Boss' new cologne. While you may be able to get the sample at a perfume counter, you are able to have the cologne sent to your house--your private data is at least worth the price of a stamp, an envelope, and a few seconds of an employees time. Admittedly, individuals who have already given up much of their data may not command a good price for any remaining information, since businesses may already have a good profile of the consumer's tastes and spending habits. However, so long as tastes, lifestyle, and spending habits change over time, and competitors do not share data with one another, a data market will always exist for even the most compromised consumers--at least, you may be able to get some free samples delivered to your door.

privacy escrow, the privacy escrow adds these costs to the price the data subject pays for anonymous transactions.

5. A Model Privacy Escrow Transaction

To explain how the privacy escrow would facilitate secured consumer transactions, I will describe a pair of fictitious purchases through Amazon.com--one without a privacy escrow, and one facilitated by a privacy escrow--focusing only on the private data transferred to the retailer. Suppose that I decided to purchase Professor Charles Whitebread's book, *The Eight Secrets of Top Exam Performance in Law School*.[49] Amazon.com requires me to furnish my name, my mailing address, my telephone number, my email address, and credit card information to complete the transaction. In addition, Amazon.com has logged my searching and browsing activity, recording my taste in books. When Amazon.com greets me at its main page ("Season's greetings, rosegary@student.law.ucla.edu"), it knows to target me as a buyer of books within a narrow category.[50] Based on

---

[49] CHARLES H. WHITEBREAD, THE EIGHT SECRETS OF TOP EXAM PERFORMANCE IN LAW SCHOOL (1995).

[50] I do not intend to portray all online profiling as inherently sinister. Many consumers do not mind if a web site is targeted to their preferences, as e-retailers are quick to point out. Of course, online businesses tend to exaggerate consumer acceptance of profiling. In one comic exaggeration, a recent IBM E-business Solutions commercial, a test group of consumers sits around a conference table complaining that businesses don't know them. One childless man complains that he receives mailers for children's clothes, a woman complains that she receives ads for auto insurance, even though she takes the subway rather than drives a car, and another woman complains that she receives ads for aluminum siding from companies that do not realize she lives in an apartment. The man complains to the marketing observers on the other side of a one-way mirror, "You're the ones with all the computers and databases.... You don't know who we are," as though he wished they did. During the commercial a "The King and I" song accompanies the dialogue with the words "Getting to know you/Getting to know all about you ...." Some isolated profiling is relatively benign, as when a single company uses past purchases to determine what kind of toy a person might want to buy. In a more troubling scenario, the information on toys is combined with data gathered from many other sites, forming an uncomfortably detailed composite of the consumer. Amazon.com has a clever way (among many) of determining customer preferences for targeted marketing. Consumers may create a "wish list" for holiday gift-giving at Amazon .com, by browsing through their various wares and selecting items that one would like to receive as a birthday present or as a holiday gift. The customer is then asked to supply friends and relatives email addresses (as

catalogued purchases made by others, Amazon.com is also able to suggest other titles that may be of interest ("People who bought *x* also bought *y*").

Now suppose that, based on my performance on my Federal Income Tax final, I believe that Professor Whitebread's suggestions were deficient and caused me to receive a lower grade than I deserved. Returning to Amazon.com, I decide to buy *Getting to Maybe: How to Excel on Law School Exams*,[51] which I am sure will provide me with the real exam secrets that Professor Whitebread refused to divulge. This time, however, I will complete the transaction using a privacy escrow agent. By using a privacy escrow agent, the transaction could be anonymous. Under a privacy escrow system, I would pay a small fee (say a few cents for a transaction,[52] or, perhaps a monthly user fee). I would have previously furnished the privacy escrow with all necessary credit card information and shipping information. The privacy escrow would agree to keep all information private and inaccessible to third parties. The privacy escrow would assign me a transaction code (for payment purposes) and a routing code (for shipping purposes) for a transaction, with each transaction requiring a new set of codes. By agreement, the privacy escrow would coordinate the use of the transaction numbers with businesses, and would coordinate use of the routing number with shippers.[53]

I would log into Amazon.com though the escrow agent's site (similar to logging on through the Anonymizer system) or through a

---

well as your own) so that they can receive the list, conveniently linked to Amazon.com to facilitate purchases. When the customer returns to the site, Amazon is able to use the information to peddle similar products (obviously hoping to fatten the wish list).

[51] RICHARD MICHAEL FISCHL & JEREMY PAUL, GETTING TO MAYBE: HOW TO EXCEL ON LAW SCHOOL EXAMS (1999).

[52] The privacy escrow need not charge much to both effectively ensure privacy and turn a healthy profit. The major investment will be in technology, not actual human monitoring of online transactions.

[53] With businesses, the privacy escrow would simply purchase products under its own account after securing funds from the customer. The business would receive a routing number from the privacy escrow, and would affix it to the product just as they would a mailing label. The shipper, by agreement with the privacy escrow, would pick up the package and rout it to the customer after receiving the code matching the routing number with the customer's address (a process that would be accomplished through secured databases). The shipper would be under contract, as would the privacy escrow, to maintain the secrecy of the routing codes.

software plug-in using an existing browser. No browsing activity would be traceable to my account. As I "proceed to check-out" (Amazon's term) with *Getting to Maybe*, I would type in the transaction code and the routing code,[54] and the privacy escrow would then debit my account, including the privacy premium, and credit the Amazon's account. Amazon would then receive a routing code from the privacy escrow, and would ship the package through FedEx, UPS, or another carrier. The carrier would receive shipping information based on the routing code from the privacy escrow, and "Getting to Maybe" would arrive at my door in time for my Corporate Finance final. Amazon.com (or those companies that Amazon may share information with) would retain no personal data as a result of the transaction.

Having briefly outlined the functions of the privacy escrow, I now move to the central question of how the privacy market and the privacy escrow system address both EU privacy requirements and U.S. policy preferences. In Part II, I will describe the EU Directive in more detail, and will explain how the privacy escrow system exceeds the requirements of the Directive. In Part III, I will describe the U.S. self-regulatory regime, and how the privacy escrow system offers a market response superior to the Safe Harbor Principles.

II. THE PRIVACY ESCROW SOLUTION SATISFIES EUROPEAN UNION PRIVACY DEMANDS

A. *The European Union Directive on Data Protection*

The European Union responded to data protection concerns through the development of an omnibus privacy policy. The European

[54] Some technical magic, beyond my skills to create or describe, will be required to make it through the data entry maze that consumers usually travel when purchasing online. While the privacy escrow may use a system similar to the Mondex or ECash system for payment (except that instead of using a single transaction number, the customer may enhance anonymity by using a random transaction number linked to this account), the business must still be willing to reconfigure their data input interfaces to accept routing numbers from the privacy escrow, instead of full addresses.

data protection policy model focuses on citizens' rights to "information self-determination,"[55] rather than on a more business-oriented self-regulatory or market-based approach. The European Union member states[56] harmonized their various data protection regulations through a five-year negotiation process, culminating in the Directive, and scheduled implementation of the Directive over three additional years.[57] The European Model has become the blueprint for various national schemes to insure privacy protection.[58]

Among the crucial features of the Directive are two provisions requiring that personal data of European origin receive "adequate" protection, be treated according to EU guidelines,[59] and, if the data do not receive adequate protection, that EU member states may prohibit data exports to the outlaw country or outlaw businesses within the country.[60] U.S. companies, who are already heavily invested in the data market and hope to avoid the exercise of these provisions by EU member states, have expressed concern over the EU "adequacy" standard, inquiring as to how they are to satisfy the standard. The U.S.

---

[55] Reidenberg, *supra* note 10, at 782 n.53. Reidenberg reports that the term "information self-determination" was coined by a German court in 1983, when it prohibited the "intrusiveness of a national census." *Id. See* Judgment of the First Senate [Bverfge, Karslruhe], Dec. 15 1983, *translated in* 5 HUM. RTS. L.J. 94 (1984).

[56] The EU member states are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the U.K.

[57] The implementation process has encountered difficulties, as the European Commission decided to send reasoned opinions to nine member states for failure to notify all the measures necessary to implement the Directive. If the Member Sates do not offer a satisfactory response to the opinions, the Commission may decide to refer the cases to the European Court of Justice. *See* The European Union Web Site, *Data Protection: Commission Decides to Send Reasoned Opinions to Nine Member States* (visited Sept. 26, 1999) <http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gttext+gt&doc+IP/99/592|0|RAPID &lg=EN>.

[58] *See* Reidenberg, *supra* note 10, at 786.

[59] *See Directive, supra* note 1, art. 4 (dealing with choice of laws), art. 25 (covering export prohibitions). To determine whether data protection is adequate, EU member state privacy commissioners are to take particular account of "the nature of the data, the conditions of a specific planned transfer, and the type of protection offered by both the legal order and the relevant business practices in the receiving nation." Schwartz, *supra* note 5, at 485 (1995); *see also Directive, supra* note 1, art. 25(2).

[60] The U.S. might successfully challenge this provision under the WTO. *See* PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN DIRECTIVE 188-96 (1998).

Department of Commerce has responded by producing the Safe Harbor Principles[61] in consultation with some of these businesses, the Principles serving as a guide to U.S. companies seeking to comply with the Directive.

B. *The Privacy Market Response*

The European imperative, though concerned primarily with rights rather than market interests, is not necessarily at odds with a market response. However, a self-regulatory response, like the Safe Harbor provisions, will take some time to implement. Furthermore, even if the Safe Harbor Principles satisfy the EU, they may not satisfy some EU Member State citizens, who may prefer a higher level of data protection. The privacy market offers many advantages to the EU and its member states' citizens that address these concerns.

First, the privacy market solution, a privacy escrow service, would immediately satisfy the European informational rights imperative. A privacy escrow allows the data subject to control her own data by completely limiting data transfer to U.S. companies, regardless of whether these companies offer adequate data protection under Directive standards.

Second, Europeans could enjoy more data control under the privacy escrow system than they receive under the consumer-friendly European Directive. The privacy escrow allows a consumer to essentially shut off the flow of all personal data, except to the privacy escrow itself. Instead of offering data security, the privacy escrow offers transactional anonymity.[62]

Third, privacy escrows may operate as European business entities, thereby keeping all private data within European borders. Using a European privacy escrow obviates concerns over potential trade disputes related to the enforcement of data export prohibitions.

---

[61] *See infra* Part III.

[62] The EU hopes to give consumers the opportunity for anonymous Internet transactions. *See* European Commission, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Anonymity on the Internet*, XV D /5022/97 Final (1997).

Fourth, because a small number of privacy escrow services could serve as the conduits for all Internet transactions, the member state Privacy Commissioners, who enforce the Directive provisions, could easily monitor proper data handling.[63] Privacy Commissioners could develop an effective regulatory relationship with a few common privacy escrows, eliminating much of the economically wasteful bureaucracy needed to monitor and enforce Directive compliance among thousands of businesses across the member states and in foreign countries. Easy enforcement is crucial to insure that the anonymity of Internet transactions does not compromise public policy initiatives against illegal content, copyright infringement, and financial fraud.[64] Clearly, the integrity of the privacy escrow service requires specific contractual provisions that prohibit the use of the service for these purposes. If the client uses the services for these purposes, the privacy escrow's contractual duty to maintain client anonymity would dissolve.

Finally, the privacy escrow system addresses some fundamental weaknesses in the European Union regulatory scheme itself. One regulatory concern is that the Directive requires equivalent protection within the European Union, but merely adequate protection outside the European Union. A European scholar, Peter Dippoldsmann, has noted that this protection discrepancy produces higher risk for EU Member State citizens since they are less likely to know how their data will be used outside the EU than in other EU member states.[65] A privacy escrow system, on the other hand, assures its clients a common standard of protection.

Also, third nations and online businesses may undermine the EU's data control capabilities by the creation of a "'data haven'--the

---

[63] According to Michael Froomkin,

> [d]ata protection laws are likely to work best when the data collectors are few, or operate in industries that are already highly regulated, such as banks. Bigger databases are easier to regulate than many small databases: the more concentrated the profile data, the greater the privacy that is possible by regulation.

Froomkin, *supra* note 17, at 490-91 (citations omitted).

[64] *See id* at 5.

[65] Peter Dippoldsmann, *Europaische Union und Datenschultz*, 27 KRISTICHE JUSTIZ 369, 377 (1994).

information equivalent of a tax haven--a single nation that offered to warehouse offshore data."[66] Although a good deal of European personal information may have escaped European borders, EU Member State citizens could impede the creation or enhancement of the data haven by cutting off data flows through the services of a privacy escrow.

III. THE PRIVACY ESCROW SYSTEM SATISFIES U.S. MARKET PREFERENCES

A. *Self-Regulation*

The U.S. position on privacy and information regulation has been to rely on market discipline to enforce adequate privacy standards, rather than to legislate a comprehensive set of privacy standards.[67] The Clinton Administration has stated that it will defer to industry self-regulation so long as the industry moves toward "effective privacy protection."[68] The Federal Trade Commission (FTC) regards self-regulation as "the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[69]

Self-regulation has had limited success. Online businesses are now providing more notice of their data practices than they were in 1998, and several "significant and promising"[70] self-regulatory privacy seal programs, such as TRUSTe[71] and BBBOnLine,[72] are now

---

[66] Froomkin, *supra* note 17, at 491; *see also* Schwartz, *supra* note 5, at 484.

[67] However, Commerce Secretary William Daley recently warned online businesses to self-regulate or risk government intervention. *See* Brad Wright, *Commerce Chief Issues Privacy Warning for Web Firms*, CNN.com (Nov. 9, 1999) <http://cnn.com/TECH/computing/9911/09/online.profiling/index.html>.

[68] *See Framework*, *supra* note 7, at 14 ("We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy.").

[69] FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (1999) [hereinafter SELF-REGULATION].

[70] *Id.*

[71] The TRUSTe program "requires participants to post an online privacy policy that meets TRUSTe guidelines, to submit to TRUSTe oversight, and to cooperate with TRUSTe's

underway. Nevertheless, "despite the laudable efforts of industry leaders,"[73] several recent assessments[74] show that the majority of web sites have not implemented the basic FTC information practices of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity.[75]

Because the self-regulatory scheme depends on fair dealing by online businesses who generally enjoy valuable leverage against consumers in the data market, privacy enthusiasts and consumer groups suspect that self-regulation will never live up to its promises. The privacy market, on the other hand, does not depend on self-

---

dispute resolution efforts. In return, participants are given the right to display TRUSTe's seal on their home page." Online Privacy Alliance, *OPA White Paper: Online Consumer Data Privacy in the United States*, at 20 (Nov. 19, 1998). OPA is an industry coalition of global corporations "concerned with protecting the privacy of individuals online." *Id* at 1.

[72] BBBOnLine is a subsidiary of the Better Business Bureau, and offers a privacy seal program similar to the TRUSTe program.

[73] SELF-REGULATION, *supra* note 69, at 6.

[74] As Joel Reidenberg discusses, there are several challenges to the development of comprehensive U.S. privacy laws. One challenge is that no existing U.S. agency or department is suited to act as a "consensus builder, privacy arbitrator, and international advocate." Reidenberg, *supra* note 10, at 790. Reidenberg suggests the creation of an independent privacy commission. *See id* at 791. Two 1999 studies indicate the current extent of self-regulation practices. The first study, the Georgetown Internet Privacy Policy Survey, lists findings from 361 of the busiest web sites on the World Wide Web. The second study, conducted by the Online Privacy Alliance, surveyed the top 100 World Wide Web sites. The graph below, produced by the Federal Trade Commission, reports the results:

	GIPPS Report	OPA Study
Number of sites in sample	361	100
Number of sites collecting personal information	337	99
Percent of sites in sample collecting personal information	93%	99%
Number of sites posting any privacy disclosure	238	93
Percent of sites in sample posting any privacy disclosure	66%	93%
Number of sites posting a privacy policy notice	157	81
Percent of sites in sample posting a privacy policy notice	44%	81%
Number of sites posting a disclosure for all four FTC substantive fair information practice principles	36	22
Percent of sites in sample posting a disclosure for all four FTC substantive fair information practice principles	10%	22%

[75] *See* Privacy Online, *supra* note 3, at 7-11.

regulation and fair dealing by data marketers--the data subject controls the data transfers herself.

B. *The Safe Harbor Principles*

Because of electronic commerce pressures[76] and political pressures developing since the creation of the Directive, U.S. companies do not enjoy the luxury of a slowly developing self-regulatory system such as they currently enjoy in the domestic market. As noted, the Department of Commerce, in consultation with many of the largest data market players, has been working on the International Safe Harbor Privacy Principles[77] in order to speed the development of the self-regulatory regime and to alleviate U.S. business concerns over the EU Directive on Data Protection. The Safe Harbor Principles "are intended for use solely by U.S. organizations receiving personal data from the European Union[78] for the purpose of qualifying for the safe

---

[76] The EU has allowed data transfers to continue while the U.S. and the EU negotiate the Safe Harbor Principles. However, U.S. companies risk losing market share to companies in countries that offer adequate and dependable data protection. European consumers, like U.S. consumers, will likely be unwilling to shop through a company that sells their personal data when they can purchase an equivalent product from a company that does not. And, if no other equivalent products are available online, an individual may decline to purchase the product, or decide to purchase through conventional means via local dealers.

[77] *See supra* note 8.

[78] *See* Safe Harbor Principles, *supra* note 8. In other words, U.S. consumers would not receive privacy protections offered under the Safe Harbor Principles. In a March 1999 address before Information Technology Association of America, Under Secretary of Commerce David Aaron said that "[i]n no way does the U.S. government intend for these safe harbor principles to be seen as precedents for any future changes in the U.S. privacy regime. Indeed, some of these principles might not be appropriate in a strictly American context." David L. Aaron, Remarks before the Information Technology Assoc. of America Fourth Annaual I.T. Policy Summit (March 15, 1999), *available at* <http://www.ita.doc.gov/media/Itaapr31599.htm> (visited Apr. 9, 2000). When the DOC solicited comments on the Safe Harbor Principles, consumers uniformly expressing displeasure with the limitation of the Safe Harbor Principles to EU citizens. A sampling of comments: "It is appalling to me that in the United States of America, land of freedom and supposed world leader in the promotion of democracy, the concerns of the citizen are subordinated to the fleeting and socially irresponsible commercialism of American businesses.... The U.S. should be embracing the standard of individual right to privacy set by such countries as those of the EU and others" [Derck Birdwell]; "I support the European, and now, Canadian, position that protects individuals' privacy on the Internet. While businesses

harbor and the presumption of 'adequacy' it creates."[79] The basic elements of the Safe Harbor Principles reflect OECD guidelines: notice; choice; onward transfer (disclosure to third parties must be consistent with notice and choice); security of data; data integrity; data subject access to their data; and enforcement mechanisms for ensuring compliance with the principles. Despite a superficial categorical similarity to the OECD guidelines, however, a number of groups have criticized the Safe Harbor Principles for their lack of substantive privacy protection.[80] The Transatlantic Consumer Dialogue (TACD), an international consumer group, urged the European Commissioners and the Ministers of the European Council to reject the Safe Harbor proposal, since they find that the proposal "lacks an effective means of enforcement and redress for privacy violations[,] places unreasonable burdens on consumers and unfairly requires European citizens to sacrifice their legal right to pursue privacy complaints through their national authorities."[81]

The most recent draft of the Safe Harbor Principles mentions only a couple of substantial remaining disagreements between the U.S. and the European Union. The European Union does not agree with the "choice" principle as outlined in the Safe Harbor proposal, since they believe the formulation offers data subjects "substantially less control

---

may complain that they should be allowed to regulate themselves--I say 'hogwash!' Just consider a moment how conscientiously businesses regulate themselves when it comes to the almighty dollar--about as much as a hog regulates its feeding at the feeding trough!" [Luca Lepori]; "I wish to state that I am strongly opposed to the policy that depends on industry self-regulation and that gives U.S. consumers less protection than European consumers. If you really believe that industry will self-regulate adequately, I have a bridge to sell you. And if you continue to promote the Safe Harbor policy, I have to assume that my tax-payer dollars are going straight into the pockets of industry, to my detriment. And, that your role of protecting consumers is being abdicated." [Cathleen Caffrey]. Comments on Safe Harbor Received From Individuals (visited on Apr. 9, 2000) <http://www.ita.doc.gov/td/ecom/599comments.htm>.

[79] *Id.*

[80] The European Union also criticized the preliminary Safe Harbor proposal. *See* Working Party of the European Data Protection Supervisory Authorities, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, DG XV D/5025/98/WP12 (July 24, 1998) <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp12en.htm>.

[81] Transatlantic Consumer Dialogue, *Recommendations on Electronic Commerce* (visited Sept. 30, 1999) <http:www.tacd.org/meeting2/electronic.html>.

of their data in comparison to the situation in Europe."[82] The second disagreement concerns the treatment of sensitive data. The Safe Harbor Principles state that:

> For sensitive information, (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual) [data subjects must be given affirmative or explicit (opt in) choice if the information is to be used for a purpose other than those for which it was originally collected or disclosed to any type of third party other than those already notified to the individual, or used or disclosed in a manner other than as subsequently authorized by the individual through the exercise of opt in choice.[83]

The European Union wishes to change the word "specifying" in the first line of the paragraph to "revealing." The Commerce Department and the businesses it represents believe that the word "revealing" "is not clear enough, because it allows so much in the way of inference."[84]

C. *The Privacy Market Solution*

The Safe Harbor Principles represent a small step toward a workable data protection scheme. However, because the Safe Harbor Principles rely on self-regulation among thousands of businesses, they do not represent a comprehensive, consumer-controlled or even especially consumer-involved solution to privacy concerns, and likely will not and cannot warrant the same level of consumer confidence as consumers would enjoy with a privacy escrow.

The privacy escrow system satisfies U.S. preferences in three ways. First, the Clinton Administration and the U.S. Department of Commerce would be satisfied that market forces, rather than omnibus

---

[82] *See* Dep't of Commerce, International Safe Harbor Privacy Principles n.2 (visited Apr. 9, 2000) <http://www.ita.doc.gov/ecom/Principles1199.htm> (draft of Nov. 15, 1999).

[83] *Id.*

[84] *Id* at n.3.

legislation, achieved a satisfactory privacy solution. Online businesses, the losers in the privacy market (to the extent that private data is no longer free), will have no standing to complain about the privacy solution. After all, these businesses have not publicly expressed concern over their own profits from data collection--they simply argued that market forces should determine the future of data privacy. Although the privacy market is not their anticipated solution to privacy concerns, it nevertheless responds to the basic market imperative demanded by U.S. government and industry, without sacrificing basic privacy imperatives demanded by consumers and the European Union.

Second, as noted above, because the privacy escrows could operate out of an EU member state, European consumers could enjoy access to U.S. online business without concern over whether the particular business adhered to the Safe Harbor Principles. The privacy escrow solution thus allows the continued development of transatlantic online markets without requiring reluctant European consumers to trust U.S. businesses' use of their private data. Since European customers may have the opportunity to deal with a local privacy escrow, they need not even send their private information across their own borders.

Finally, the privacy escrow system also offers U.S. consumers the same protection as their European counterparts. U.S. consumers, like European consumers, need not worry about whether Amazon, Disney, or Microsoft will abide by the Safe Harbor provisions. The privacy market response offers is not simply a market response to the difficulties posed by EU/U.S. data protection differences, but is a solution to privacy concerns between any data subject and any data recipient.[85]

[85] Note, however, that some personal data *must* be collected for certain transactions (e.g., insurance policies). The privacy escrow will be of limited value in these situations. Consumers may need to rely on model contracts with data collectors in these rare instances. These data transfers typically include explicit contractual agreements, and thus the incorporation of a model contract in these instances would not burden the transaction.

IV. CONCLUSION

The creation of a privacy market through the privacy escrow system represents an immediately workable solution to EU/U.S. differences on privacy and data protection. The privacy escrow system would allow consumers to transact with online businesses anonymously, whether through email, browsing, or purchases. The ability to transact anonymously exceeds any self-regulatory scheme currently in development, including the Safe Harbor Principles, and easily satisfies the demands of the European Union Directive on Data Protection. Also, because a privacy escrow system does not require legislative intervention, but represents an entirely industry-generated solution to the problems of data transfers, it satisfies the U.S. preference for a market response.

As U.S. data marketers frequently mention, electronic commerce can only flourish if allowed to develop without restraining legislation. As privacy enthusiasts counter, the development of e-commerce is presently hampered by public fear over the uses of private data transferred through online transactions. The privacy escrow solution responds to both concerns, offering a market response that fosters consumer confidence in electronic commerce.